From the Peace Corps spokesperson:

The President issued Executive Order 13587 to improve the security of classified computer networks and classified material. As part of the EO, the President directed federal departments and agencies with classified networks to establish insider threat detection and prevention programs, and the Peace Corps has identified a senior official to oversee implementation of these programs.

The President established the National Insider Threat Task Force under joint leadership of the Attorney General and the Director of National Intelligence to assist agencies in developing and implementing their insider threat programs, and the Peace Corps is working in coordination with the Task Force to ensure the security of classified networks and the responsible sharing and safeguarding of classified information.

In developing standards for these programs, the Task Force specifically sought to develop standards that do not erode civil liberties, civil rights, or privacy protections for government employees. For more details, I direct you to the ODNI.

Questions from McClatchy:

1. Did your self-assessments determine that your agency's safeguards against UDs were inadequate? If so, what corrective actions were taken and improvements realized?

2. Has your agency identified any other "insider threats" as part of your new definition other than leaking classified information? You mentioned in the last response the need for protecting sensitive information. Does the Peace Corps see sensitive, but unclassified or For Official Use Only as an insider threat risk or violation? Other agencies have identified other insider threats that are unique to their agencies.

3. The Minimum standards call for employee training of the insider threat, specifically with the recognition of insider threat behaviors. Can we have copies of the training materials? How about the list of behaviors?

4. The Insider Threat point person in each agency is going to have access to a wide range of departments that don't include only security, such as human resources. How do you ensure that someone who goes to human resources for a personal issue is not then turned in to the Insider threat official.

For example, someone says they have a personal issue that is part of the behavior for an insider threat. My understanding is that human resources would then have to pass along that information to the Insider Threat official. If so, how does your agency handle that kind of case?

5. Did you agency have to create this program from scratch? If not, what pre-existing office/program are you working with?

6. How many UDs have been reported since your agency began implementing this? If not reporting yet, why not?

7. Have your efforts resulted in increased detection of UDs? If so, how does your agency determine whether they should be handled administratively or referred for criminal investigation?

8. Has your agency encountered any specific problems or objections to implementing the EO? If so, what have they been?

9. Can we get copies of the guidance and standards that your agency has developed for insider threat detection?

10. Can you provide us with your self-assessments or summaries of the assessments?

11. How will you be handling the reporting process by co-workers logistically? Is there going to be a 800 number? Or, Internet reporting?